CLAIMS FROM THE ORIGINAL PCT APPLICATION (16 June 2000)

1 . Process of securing the access to a data processing server from a client site through at least a first communication network, this server comprising means for handling a protocol of authenticating a client site user, comprising a sequence of identification data receiving and processing, and a sequence of transmitting a message from the server site to a client site user owned communication equipment through a second communication network, characterized this transmitted message is a voice message foreseen to be directly processed by the aforesaid user for generating an authentication password intended to be transmitted to the aforesaid server site through either of the first or second aforesaid communication networks.

2 . Securing process according to claim 1, characterized in that it comprises steps of:

- requesting identification data (ID, MPC) from the client site through the first communication network (4);
- processing the aforesaid data (ID, MPC) and searching an authentication data base (BDA) for a client user owned mobile communication equipment call number;
- calling the aforesaid communication equipment through at least a second communication network;
- after establishing a communication with the aforesaid mobile communication equipment, generating a random or pseudo random password (MPA);

- sending a voice message comprising the aforesaid random password through the second communication network (6);
- requesting the user to provide, from the client site through the first communication network (4) an authentication password (MPAUT) derived from the aforesaid random or pseudo random password (MPA); and
- authenticating the aforesaid authentication password (MPAUT).

3 . Process according to claim 2, characterized in that the authentication password (MPAUT) matches the server generated random or pseudo random password (MPA) transmitted through the mobile communication equipment.

4 . Process according to claim 3, characterized in that the authentication password (MPAUT) is built from the random or pseudo random password (MPA) generated by the server and transmitted through the mobile communication equipment, applying a client user known and embodied within the server authentication data base (BDA) key, the authentication step comprising a step of converting the aforesaid authentication password into a random or pseudo random authentication password (MPA) by applying the aforesaid key.

5 . Process according to any of the previous claims, characterized in that the identification data requested from the client consists of a couple [identification code/client password] (ID/MPC).

6 . Process according to any of the previous claims, characterized in that the step of requesting the authentication password (MPAUT) from the user takes place during a predetermined time-out delay beyond which the authentication is denied.

7 . Securing process according to claim 1, characterized in that it comprises on the server side the steps of:

- requesting authentication data (ID, MPC) from the client site through the first communication network (4);
- processing the aforesaid data (ID, MPC) and searching an authentication data base (BDA) for a client site user owned mobile communication equipment call number;
- calling the aforesaid communication equipment through at least a second communication network;
- in case the communication is established with the aforesaid mobile communication equipment, send a voice message requesting the user to send an encryption key;
- receiving and recognising the encryption key transmitted by the client by means of the mobile equipment keyboard,
- deciphering by means of the aforesaid encryption key an authentication password (MPAUT) transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and
- authenticating the client password (MPC) which results from the authentication password deciphering.

8 . Process according to claim 7, characterized in that the step of receiving the encryption takes place during a predetermined time-out delay beyond which the authentication is denied.

9 . System of securing the access to a data processing server through at least a first communication network, which implements the process according to either of the previous claims, this system comprising at the server site

means for handling a protocol of authenticating of a client site user, means for generating and transmitting through a second communication network a message from the server site to a client site user owned mobile communication equipment, characterized in that the system is laid out for transmitting through the second communication network a voice message foreseen to be directly processed by the aforesaid user for generating an authentication password intended to be transmitted to the aforesaid server site through the first communication network.

10 . Securing system according to claim 9, further comprising:

- means for searching an authentication data base (BDA), in response to identification data received from an access requesting client site, a client site user owned mobile communication equipment call number;
- means for calling this communication equipment through at least a second communication network;
- means for generating a random or pseudo random password (MPA); and
- means fro authenticating an authentication password incoming from the client site, characterized in that the system further comprises:
- means for sending a voice message comprising the aforesaid random password (MPA) through the second communication network, and
- means for requesting the client site user to provide, through the first communication network (4), an authentication password (MPAUT) derived from the aforesaid random or pseudo random password (MPA).

11 . Securing system according to claim 9, further comprising:

- means for requesting the client site for identification data (ID, MPC) through a first communication network (4);
- means for processing the aforesaid data (ID, MPC) and for searching an authentication data base (BDA), in response to identification data received from an access requesting client site, a client site user owned mobile communication equipment call number;
- means for calling this communication equipment through at least a second communication network;
- means for calling the aforesaid communication equipment through at least a second communication network,
- means for sending a voice message which requests the user to send en encryption key,
- means for receiving and recognising the encryption key entered by the user by means of his mobile communication equipment keyboard,
- means for deciphering by means of the aforesaid encryption key an authentication password (MPAUT) transmitted by the client through the first communication network, this password resulting from the encryption of a client password performed at the client site by means of the encryption key; and
- means for authenticating the client password (MPC) which results from the authentication password deciphering.

12 . Application of the securing process according to any of the 1 to 8 claims in a system for authenticating digital creations comprising third parties of time stamping, authentication and archiving connected to a first communication network, characterized in that each third party site locally comprises software means (i) for transmitting securing data in voice form to a client site which requests an authentication operation, through a mobile communication equipment attached to the aforesaid client site and connected to a

second communication network, and (ii) for receiving through the first communication network an authentication password resulting from the aforesaid securing data.